IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with <u>underlining</u> and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1.   (currently amended) An extended key preparing apparatus wherein extended keys are prepared in common key cryptosystem from a cryptographic key input, comprising:

a dividing unit which divides ~~binary digit~~ <u>a bit</u> string of said cryptographic key into a plurality of ~~elements each composed of~~ <u>bit groups, each bit group having</u> a predetermined bit length;

an intermediate data preparing unit which prepares a plurality of intermediate data ~~by applying a plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing unit~~<u>groups from the bit groups by a predetermined operation with different constant for each bit group, each intermediate data group having first intermediate data</u>;

a selecting unit which selects ~~a plurality of~~ <u>one item of the first</u> intermediate data ~~corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing unit~~<u>for each of the intermediate data groups depending on a number of stages of extended keys to determine second intermediate data</u>; and

an extended key preparing unit which prepares the extended keys ~~corresponding to said number of stages~~ <u>having a bit length longer than the bit string of said cryptographic key</u> by converting irreversibly the ~~plurality of the~~<u>second</u> intermediate data ~~selected by said selecting unit.~~<u>, wherein said intermediate data preparing unit is provided with a nonlinear type operating unit for effecting a nonlinear type operation with respect to each bit group to prepare the intermediate data groups.</u>

2.   (canceled)

3.   (currently amended) An extended key preparing apparatus according to claim ~~2~~ <u>1,</u> wherein said ~~nonlinear type operating unit performs nonlinear type operation in such a manner that when said cryptographic key is divided into eight elements of 32 bits by said dividing~~

~~unit,~~dividing unit divides the bit string of said cryptographic key into eight of the bit groups, the predetermined bit length is 32 bits, and said nonlinear type operating unit separates ~~said~~ ~~elements~~ each bit group into 6, 5, 5, 5, 5, and 6 bits to transpose the same into other data, respectively, and the data after transposition are subjected to nonlinear type operation by the use of a determinant.

4. (currently amended) An extended key preparing apparatus according to claim ~~2~~ 1, wherein said intermediate data preparing unit is provided with:

an addition unit which adds a first constant to an ~~odd-number-th element~~ even-numbered bit group that has been subjected to the nonlinear type operation to obtain a first result;

a multiplication unit which multiplies by a second constant an ~~even-number-th element~~ odd-numbered bit group which has been subjected to the nonlinear type operation ~~by said~~ ~~constant~~ to obtain a second result, wherein the odd number is the even number plus one; and

an exclusive OR operating unit which effects exclusive OR operation of ~~said odd-number-~~ ~~th element to which has been added the constant and said even-number-th element which is~~ ~~succeeding to said odd-number-th and to which has been multiplied by said constant~~ the first result and the second result.

5. (currently amended) An extended key preparing apparatus according to claim 4, comprising further a preparing unit for preparing the intermediate data group by ~~subjecting~~ ~~nonlinear-type operation to the~~ nonlinearly operating on a result of said exclusive OR operation ~~of said odd-number-th element and said even-number-th element which is succeeding to said~~ ~~odd-number-th~~.

6. (currently amended) An extended key preparing apparatus according to claim 5, wherein said addition unit and said multiplication unit repeat ~~the~~ a plurality of times additions and multiplications by the use of the number i of different constants, respectively, to prepare the number i of data in every ~~elements~~ bit group; said exclusive OR operating unit ~~repeat~~ repeats i times operations for acquiring exclusive OR of the ~~odd-number-th element~~ even-numbered bit group and the ~~even-number-th element~~ odd-numbered bit group which have been operated by the use of the same constants; and said preparing unit prepare the number i of items of the first intermediate data in every ~~elements~~ bit group.

7.   (currently amended) An extended key preparing apparatus according to claim 6, wherein said selecting unit selects one <u>item of the first</u> intermediate data corresponding to said number of stages of an extended key among the number i of <u>items of the first</u> intermediate data contained in the respective ~~elements~~ <u>intermediate data groups</u> which have been prepared by said intermediate data preparing unit.

8.   (currently amended) An extended key preparing apparatus according to claim 1, wherein said extended key preparing unit is provided with:

a rearrangement unit which rearranges ~~a plurality of~~ <u>the second</u> intermediate data ~~selected by said selecting unit~~ <u>to obtain a rearranged intermediate data</u>; and

an irreversible conversion unit which converts irreversibly ~~the plurality of intermediate data that have been rearranged by said rearrangement unit~~ <u>the rearranged intermediate data</u>.

9.   (currently amended) An extended key preparing apparatus according to claim 8, wherein ~~when intermediate data are rearranged in an order of elements X, Y, Z, and W by said rearrangement unit,~~ <u>the second intermediate data includes four items represented by four elements X, Y, Z, and W, respectively,</u>

<u>said rearrangement unit rearranges the four items, and</u>

said irreversible converting unit prepares a first data by adding the element Y to a data obtained by shifting cyclically the element X leftwards by 1 bit; prepares a second data determined by sifting cyclically the data leftwards by further 1 bit, which data has been obtained by subtracting the element W from a data obtained by shifting cyclically ~~said~~ <u>the</u> element Z leftwards by 1 bit; and ~~operates~~ <u>performs an</u> exclusive OR ~~of~~ <u>operation on</u> said first data and said second data.

10.   (currently amended) An extended key preparing apparatus according to claim 1, wherein said dividing unit divides a cryptographic key of 128 bits, 192 bits, or 256 bits into eight ~~elements~~ <u>groups</u> of 32 bits.

11.   (currently amended) An extended key preparing method wherein extended keys are prepared in common key cryptosystem from a cryptographic key input, comprising ~~the steps of,~~ <u>:</u>

dividing ~~binary digit~~ <u>a bit</u> string of said cryptographic key into a plurality of ~~elements~~ <u>bit</u> groups, each ~~composed of~~ <u>bit group having</u> a predetermined bit length;

Serial No. 09/811,551

preparing a plurality of intermediate data ~~by applying the plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing step~~groups from the bit groups by effecting a nonlinear type operation with different constant for each bit group, each intermediate data group having a first intermediate data;

selecting ~~a plurality of~~one item of the first intermediate data ~~corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing step~~for each of the intermediate data groups depending on a number of stages of extended keys to determine second intermediate data; and

preparing the extended keys ~~corresponding to said number of stages~~having a bit length longer than the bit string of said cryptographic key by converting irreversibly ~~the plurality of~~the second intermediate data ~~selected by said selecting step~~.

12.   (canceled)

13.   (currently amended) An extended key preparing method according to claim ~~12~~ 11, wherein ~~said nonlinear type operating step performs nonlinear type operation in such a manner that when said cryptographic key is divided into eight elements of 32 bits by said dividing step,~~said dividing includes dividing the bit string of said cryptographic key into eight of the bit groups, the predetermined bit length is 32 bits, and

said ~~nonlinear type operating step separates~~effecting of the nonlinear type operation includes separating~~said elements~~each bit group into 6, 5, 5, 5, 5, and 6 bits to transpose the same into other data, respectively, and the data after transposition are subjected to a nonlinear type operation by the use of a determinant.

14.   (currently amended) An extended key preparing method according to claim ~~12~~ 11, wherein said ~~intermediate data~~preparing ~~step involves~~of the plurality of intermediate data groups includes~~:~~

~~an addition step for~~adding a first constant to an ~~odd number-th element~~even-numbered bit group that has been subjected to the nonlinear type operation to obtain a first result;

~~a multiplication step for~~multiplying by a second constant an ~~even number-th element~~odd-numbered bit group which has been subjected to the nonlinear type operation ~~by said constant~~to obtain a second result, wherein the odd number is the even number plus one; and

~~an exclusive OR operating step for~~effecting an exclusive OR operation of ~~said odd number-th element to which has been added the constant and said even number-th element~~

5

~~which is succeeding to said odd number-th and to which has been multiplied by said constant~~<u>the first result and the second result</u>.

15.   (currently amended) An extended key preparing method according to claim 14, <u>further</u> comprising ~~further a step for~~ preparing <u>the</u> intermediate data <u>group</u> by ~~subjecting nonlinear type operation to the~~ <u>nonlinearly operating on a</u> result of said exclusive OR operation ~~of said odd number-th element and said even number-th element which is succeeding to said odd number-th~~.

16.   (currently amended) An extended key preparing method according to claim 15<u>,</u> wherein said ~~addition step~~<u>adding</u> and said ~~multiplication step~~<u>multiplying</u> ~~repeat the~~ <u>includes repeating a</u> plurality of times additions and multiplications by the use of the number i of different constants, respectively, to prepare the number i of data in every ~~elements~~<u>bit group</u>; said ~~exclusive OR operating step~~ <u>effecting of the exclusive OR operation</u> ~~repeat~~ <u>includes repeating</u> i times operations for acquiring exclusive OR of the ~~odd number-th element~~ <u>even-numbered bit group</u> and the ~~even number-th element~~<u>odd-numbered bit group</u> which have been operated by the use of the same constants; and said preparing ~~step~~<u>of the intermediate data group by nonlinearly operating</u> ~~prepare~~<u>includes preparing</u> the number i of intermediate data in every ~~elements~~<u>bit group</u>.

17.   (currently amended) An extended key preparing method according to claim 16<u>,</u> wherein said selecting ~~step selects~~<u>includes selecting</u> one <u>item of the first</u> intermediate data corresponding to said number of stages of an extended key among the number i of <u>items of the first</u> intermediate data contained in the respective ~~elements~~<u>intermediate data groups</u> which have been prepared by said intermediate data preparing step.

18.   (currently amended) An extended key preparing method according to claim 11<u>,</u> wherein said ~~extended key~~ preparing ~~step involves:~~<u>of the extended keys includes</u>

   ~~a rearrangement step for~~ rearranging ~~a plurality of~~ <u>the second</u> intermediate data ~~selected by said selecting step~~<u>to obtain a rearranged intermediate data</u>; and

   ~~an irreversible conversion step for~~ converting irreversibly ~~the plurality of intermediate data that have been rearranged by said rearrangement step~~<u>the rearranged intermediate data</u>.

19.   (currently amended) An extended key preparing method according to claim 18, wherein ~~when intermediate data are rearranged in an order of elements X, Y, Z, and W by said rearrangement step,~~the second intermediate data includes four items represented by four elements X, Y, Z, and W, respectively,

said rearranging includes rearranging the four items, and

said ~~irreversible~~converting ~~step prepares~~ includes

preparing a first data by adding the element Y to a data obtained by shifting cyclically the element X leftwards by 1 bit; prepares a second data determined by sifting cyclically the data leftwards by further 1 bit, which data has been obtained by subtracting the element W from a data obtained by shifting cyclically ~~said~~ the element Z leftwards by 1 bit; and

~~operates~~performing an exclusive OR ~~of~~operation on said first data and said second data.

20.   (currently amended) An extended key preparing method according to claim 11, wherein said dividing step divides a cryptographic key of 128 bits, 192 bits, or 256 bits into eight ~~elements~~groups of 32 bits.

21.   (currently amended) A computer readable recording medium wherein an extended key preparing program in which extended keys are prepared in common key cryptosystem from a cryptographic key input is to be recorded, the program comprising program code means which when executed perform:

~~recording the program containing a dividing step for~~ dividing ~~binary digit~~ a bit string of said cryptographic key into a plurality of ~~elements~~bit groups, each ~~composed of~~ bit group having a predetermined bit length;

~~an intermediate data preparing step for~~preparing a plurality of intermediate data groups ~~by applying the plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing step~~ from the bit groups by effecting a nonlinear type operation with different constant for each bit group, each intermediate data group having a first intermediate data;

~~a selecting step for selecting a plurality of~~ one item of the first intermediate data ~~corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing step~~for each of the intermediate data groups depending on a number of stages of extended keys to determine second intermediate data; and

7

~~an extended key preparing step for~~ preparing the extended keys ~~corresponding to said number of stages~~ having a bit length longer than the bit string of said cryptographic key by converting irreversibly ~~the plurality of~~ the second intermediate data ~~selected by said selecting step~~.

22.   (currently amended) An extended key preparing program in which extended keys are prepared in common key cryptosystem from a cryptographic key input, the program comprising program code means which when executed perform:

~~recording the program containing a dividing step for~~ dividing ~~binary digit~~ a bit string of said cryptographic key into a plurality of ~~elements~~ bit groups, each ~~composed of~~ bit group having a predetermined bit length;

~~an intermediate data preparing step for~~ preparing a plurality of intermediate data groups ~~by applying the plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing step~~ from the bit group by effecting a nonlinear type operation with different constant for each bit group, each intermediate data group having first intermediate data;

~~a selecting step for~~ selecting ~~a plurality of~~ one item of the intermediate data ~~corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing step~~ for each of the intermediate data groups depending on a number of stages of extended keys to determine second intermediate data; and

~~an extended key preparing step for~~ preparing the extended keys ~~corresponding to said number of stages~~ having a bit length longer than the bit string of said cryptographic key by converting irreversibly ~~the plurality of~~ the second intermediate data ~~selected by said selecting step~~.

23.   (new) An extended key preparing apparatus wherein extended keys are prepared in common key cryptosystem from a cryptographic key input, comprising:

a dividing unit which divides binary digit string of said cryptographic key into a plurality of elements each composed of a predetermined bit length;

an intermediate data preparing unit which prepares a plurality of intermediate data by applying a plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing unit, said intermediate data preparing unit being provided with a nonlinear type operating unit for effecting nonlinear type operation with respect

to the respective elements divided by said dividing unit, said nonlinear type operating unit performing nonlinear type operation in such a manner that when said cryptographic key is divided into eight elements of 32 bits by said dividing unit, said nonlinear type operating unit separates said elements into 6, 5, 5, 5, 5, and 6 bits to transpose the same into other data, respectively, and the data after transposition are subjected to nonlinear type operation by the use of a determinant

a selecting unit which selects a plurality of intermediate data corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing unit; and

an extended key preparing unit which prepares the extended keys corresponding to said number of stages by converting irreversibly the plurality of the intermediate data selected by said selecting unit.

24.   (new) An extended key preparing method wherein extended keys are prepared in common key cryptosystem from a cryptographic key input, comprising the steps of,

dividing binary digit string of said cryptographic key into a plurality of elements each composed of a predetermined bit length;

preparing a plurality of intermediate data by applying the plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing step, said preparing involving a nonlinear type operating step for effecting nonlinear type operation with respect to the respective elements divided by said dividing step, said nonlinear type operating step performing a nonlinear type operation in such a manner that when said cryptographic key is divided into eight elements of 32 bits by said dividing step, said nonlinear type operating step separates said elements into 6, 5, 5, 5, 5, and 6 bits to transpose the same into other data, respectively, and the data after transposition are subjected to nonlinear type operation by the use of a determinant;

selecting a plurality of intermediate data corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing step; and

preparing the extended keys corresponding to said number of stages by converting irreversibly the plurality of the intermediate data selected by said selecting step.